



***Information Technology (IT) Policies***



**020.205 IT System Technical Assessments Policy**

**Version 2.0**  
**October 21, 2015**

020.205 IT System Technical Assessments Policy	Current Version: 2.0
020.000 Managerial Security	Effective Date: 05/02/2005

## Revision History

Date	Version	Description	Author
5/2/2005	1.0	Effective Date	CHFS IT Policies Team Charter
10/21/2015	2.0	Revision Date	CHFS IT Policies Team Charter
10/21/2015	2.0	Review Date	CHFS IT Policies Team Charter

020.205 IT System Technical Assessments Policy	Current Version: 2.0
020.000 Managerial Security	Effective Date: 05/02/2005

## Table of Contents

<b>020.205 IT SYSTEM TECHNICAL ASSESSMENTS POLICY .....</b>	<b>4</b>
1.1 POLICY .....	4
1.2 SCOPE.....	4
1.3 POLICY/PROCEDURE MAINTENANCE RESPONSIBILITY .....	4
1.4 EXCEPTIONS.....	4
1.5 RESPONSIBILITY .....	4
1.6 REVIEW CYCLE .....	4
1.7 CROSS REFERENCES.....	5

020.205 IT System Technical Assessments Policy	Current Version: 2.0
020.000 Managerial Security	Effective Date: 05/02/2005

## **020.205 IT Systems Technical Assessments Policy**

Category: 020.000 Managerial Security

### **1.1 Policy**

CHFS complies with and adheres to the Commonwealth Office of Technology (COT) Policy #CIO-082, Critical Systems Vulnerability Assessments. CHFS Office of Administrative and Technology Services (OATS) works collaboratively with program areas to determine the level of sensitivity for its data. For those systems deemed critical by the program areas because of confidential data, it is the policy of this Cabinet to conduct vulnerability assessments in accordance with COT Policy CIO-082. The Cabinet also follows CHFS IT Policy 065.014. Vulnerability assessments may be performed by internal CHFS IT Security staff or contracted by approved third party assessment providers as approved by the CHFS CIO.

### **1.2 Scope**

The scope of the policy is for all systems deemed critical by the program areas because of confidential data.

### **1.3 Policy/Procedure Maintenance Responsibility**

The Cabinet for Health and Family Services (CHFS) Application Security Architect is responsible for the update of this policy as well as the associated procedures whenever change to the infrastructure or enterprise environment occurs.

### **1.4 Exceptions**

Any exceptions to this policy must follow the procedures established in CHFS IT Policy #070.203.

### **1.5 Responsibility**

CHFS Application Security Architect is responsible for oversight of vulnerability assessments of each system covered by this policy. If OATS IT Security and Audit Section uses a third party, the group is responsible to ensure that the vendor is a qualified organization as determined by COT.

### **1.6 Review Cycle**

Annual

020.205 IT System Technical Assessments Policy	Current Version: 2.0
020.000 Managerial Security	Effective Date: 05/02/2005

## **1.7 Cross Reference(s)**

- COT Enterprise Policy CIO-082 – Critical Systems Vulnerability Assessments
- CHFS IT Policy #065.014 – Division of Systems Management System Development Lifecycle
- CHFS IT Policy #070.203 – Exceptions to Standards and Policies.